DEPARTMENT OF COMMERCE · UNITED STATES OF AMERICA

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

BC8

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR		ATTORNEY DOCKET NO.
09/120,763	07/22/98	ETZEL	M	ETZEL-5-3-11

WM31/0628

PETER H PRIEST
529 DOGWOOD DRIVE
CHAPEL HILL NC 27516

EXAMINER	
SEAL, J	
ART UNIT	PAPER NUMBER
2131	9

DATE MAILED: 06/28/01

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner of Patents and Trademarks

Office Action Summary	**Application No.** 09/120,763	**Applicant(s)** ETZEL ET AL.
	Examiner James Seal	**Art Unit** 2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136 (a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 May 2001* .

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-18* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claims _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are objected to by the Examiner.

11)□ The proposed drawing correction filed on _____ is: a)□ approved b)□ disapproved.

12)□ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. § 119

13)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____ .

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)□ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. § 119(e).

Attachment(s)

15) ☒ Notice of References Cited (PTO-892)

16) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

17) □ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .

18) ☒ Interview Summary (PTO-413) Paper No(s). _____ .

19) □ Notice of Informal Patent Application (PTO-152)

20) □ Other: .

DETAILED ACTION

1. This action is in response to your correspondence of 21 May 2001.

2. Claims 1-18 are pending.

Specification

3. The disclosure is objected to because of the following informalities: page 3 paragraph 2, serial numbers should be provided.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1 -5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Reeds (EP 0532228 A2) and further in view of Laufer (Discrete Mathematics and Applied Modern Algebra).

6. In claim 1, applicant recites a method which is to be employed with a wireless telephone encryption system in which a plaintext message is introduced, one or more offset values are generated, a first transformation is performed on the message, an iteration of the CMEA (Cellular Message Encryption Algorithm) process is then performed employing an enhanced T-box function using an involutary table lookup, the

inputs of the enhanced tbox subject to permutation using one or more of the secret offsets, and finally a second transformation is applied to the message to produce an output.

7. Reeds discloses a digital cellular telephone that encrypts messages using an encryption algorithm, and thus a CMEA. Reeds further discloses a three stage encryptor (see Figure 10) and according to one embodiment, the first stage consist of autokeyed encryptor (that is, the key is derived from a portion of the message as encrypted by the encryptor, Column 3, lines 13-15), the second stage uses a one time pad encryption (that is a Vernam cipher, see Abstract line 5) composed of iterative (see Column 9, lines 45-67, consisting of initializing and updating values as the values are iterated over the integers z) self-inverting (involutions) which are implemented by an array TBOX[z] = z and a third stage is a second autokeying decryption that corresponds to the autokeyed encryption of the first stage (i.e., the inverse of the first stage, Column 9, lines 61-62), using an 8-bit microcomputer (Abstract, Column 3, lines 6-16; Columns 9, lines 13-20, lines 43, 49-50; Column 11, lines 5-12). Autokeying requires an offset, between the plaintext and the autokeyed ciphertext and thus Reeds must have at least two offsets, one for each autokeyed transformation. Multiloop autokeying would require several offsets (one for each loop). Reeds calculation are performed with an 8-bit microprocessor and thus the cryptographic functions are *discrete functions* (Column 3, line 9), that is their inputs and output are over a discrete set of integers. Reeds is silent on the use of table lookup to evaluate involutions although he does refer to the TBOX[z] as an array. Discrete functions are defined in terms of an array rather than a formula as with continous functions. Laufer (Discrete Mathematics and Applied Modern Algebra) teaches the use of tables pages 209-211) such discrete and in particular the discrete involution function page 210, viii. As such one of ordinary skill in the art would have

been motivated to have used the method of table look up for evaluating the discrete involution of Reeds. Claim 1 is rejected.

8. In claim 2, applicant recites a method with the limitations of claim 1 and with the further limitations that there are one or more secret offsets.

9. Reeds discloses at least two offsets, one for each of the autokeyed transformations. Claim 2 is rejected.

10. In claim 3, applicant recites a method with the limitations of claim 2 and with the further limitations that the step of generating the first and second offset is accomplished by combining an external value with one of a plurality of secret values.

11. Reeds discloses that the offsets depend on time (an external value, Column 10, lines 6-7) and secret values e.g. from the SSD-B subfields (lines 17-18). Claim 3 is rejected.

12. In claims 4 and 5, applicant recites the method of claim 3 with the further limitation that the secret value includes two 8-bit values for each offset and further the external value is 8-bit value.

13. Reeds discloses that the calculations are to be performed on an eight-bit processor. Claims 3 and 4 are rejected.

14. Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Reeds and Laufer as applied to claims 1 and 5 above, and further in view of Vernan (Cipher Printing Telegraph System).

15. In claim 6, applicant recite the method of claim 5 with the further limitation that the two offsets are to be calculated from the external value CS_n and the two secret

values K_0 and K_1 as follows: offset 1 = $((K_0 + 1)*CS_n \bmod 257) \oplus K_1 \bmod 256$ and offset 2 = $((K_0 + 1)*CS_n \bmod 257) \oplus K_1 \bmod 256$.

16. If one considers Reeds' second embodiment, that is, using a secret values (i.e. from the SSD-B subfield) and an external value (say corresponding to the time, Column 10, lines 6-7), to generate the two autokey offset (or a pularity of such offsets for multiloop autokeying), iterating a one time pad (a Vernam cipher AIEE, Feb 1926, pages 109 –115, in particular *Running key ciphers*, page 113, lines 21-24. Reeds differs from claim 6 in that details of Vernam's one time pad are not provided. As applied to the calculation of an offset, Reeds' two secret values K1 and K2 appear as keys and the external value appears as the quantity to be encrypted. A product of the second key with the external value (to prevent frequency cryptananalysis, page 112 column 2) is then XORed (i.e., $\oplus$) by the second key (see page 113, second column 2 lines 22-25). However, to make the key as long as possible without repetition, Vernam used two key tapes which were set up such that a complete circuit around the first tape would advanced the second tape by 1 (pages 133, and 114 both second column). Mathematically one can represent what Vernam did mechanically using paper tapes, by a modular product of the second secret value by the external value mod n and mod (n+1). The first moduli applies to the first tape and the second moduli applies to the second type and the differ in moduli to insure that one circuit around the second loop does not cause a repetition before the first loop is finished. Thus Reeds' two secret offsets are calculated in the same way as ciphertext in a one time pad. As Reeds' uses 8-bit cryptoprocessor the range of values of 0 to 256 (see Column 10, line 43) i.e., n = 256 (above) for the "tapes". The offset Reeds/Vernam differs from that recited in that K_2 is replaced by K_2 + 1, where K_2 is the second secret value. However, the examiner takes official notice that in order for the autocoder to function the offset must always be

one or more. To insure this happens, we would then add one to the second secret value. As Reeds does not provide the details of a one time pad, thus one of ordinary skill in the art would have been motivated to review the teachings of Vernam to obtain the details of the one time pad. Claim 6 is rejected.

17. Claims 7- 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Reeds, Laufer and Vernam as applied to claims 1 and 6 above, and further in view of Takaragi et. al. (5,222,139).

18. In claims 7 and 8, applicant recites a method werein the first and second transformation respectively includes bit trading and involution lookup with feedback, random byte permutation, feedback employing both the first and second secret offsets.

19. Reeds disclose the a multistage encryption system that uses discrete involution and Laufer proveds table look up to evaluate discrete functions, and feedback (see figure 5b), but are silent on specific involution transformations. Reeds does not disclose the specific types involutions. Takaragi et. al. teach the use of other discrete involutions such as bit trading (bit swapping), bit rotation, bit and bit shifting bits left or As Reeds does not provide the details of particular involutions, one of ordinary skill in the art would have been motivated to review the involutions as applied to bit streams. Claim 7 and 8 are rejected.

20. Claims 9-16 recite the corresponding decryption system to complement the encryption system recited in claims 1-8. Decryption is an essential part of a cryptosystem and as noted above the prior art discloses an encryption/decryption systems. Claim 9-16 are rejected.

21. Claim 17 recites an apparatus (a secure wireless headset or secure cellular phone) with transceiver, input/output interface, key generator for generating one or more keys and a cryptoprocessor, with an input/output interface a message to be encrypted or decrypted together with a message ID's. This is standard in any cell phone and is included in the prior art cited above. The claim recites the CMEA process , with one or more offsets, tbox, employing involutions lookup, were aready addressed in claim 1. Claim 17 is rejected.

22. Claim 18 recties a wireless base station consisting of a transceiver, input/output interface, key generator for generating one or more keys, a cryptoprocessor for encryption/decryption of messages together with message ID's. . This is standard in any base station administering to cell phones and is included in the prior art cited above. Further the claim recites a reverse enhanced CMEA processor including a first and second inverse transformation, tbox, offsets, involution lookup. These limitations have been addressed in claim 9. Claim 18 rejected.

Double Patenting

23. A rejection based on double patenting of the "same invention" type finds its support in the language of 35 U.S.C. 101 which states that "whoever invents or discovers any new and useful process ... may obtain a patent therefor ..." (Emphasis added). Thus, the term "same invention," in this context, means an invention drawn to identical subject matter. See *Miller v. Eagle Mfg. Co.*, 151 U.S. 186 (1894); *In re*

Ockert, 245 F.2d 467, 114 USPQ 330 (CCPA 1957); and *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970).

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970);and, *In re Thorington,* 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

24. Claims 1-18 of application 09120763 is an obvious variation of application 09124300 and is rejected as nonstatutory double patenting.

25. Claim 1 of '763 differs from '300 in the preamble by the use of CMEA encryption or decryption cryptoprocessing ('763) versus CMEA cryptoprocessing ('300). Encryption or decryption is inherent in cryptoprocessing. Further '763 recites performing a first transformation on the unprocessed message... and finally a second transformation on the intermediate cryptotext, while '300 recites performing a transformation on the unprocessed message... and finally an inverse transformation on the intermediate ciphertext. The examiner notes cryptotext and ciphertext are synonymous and that in '300 performing a transformation ... constitutes a first transformation and followed by performing an inverse transformation... constitutes a

second transformation thus claim 1 of '763 reads on claim 1 of '300. Thus, while the language of claim 1 ('763) differs from that of claim 1 ('300) the differences are obvious.

26. Claims 2-6 of ('300) read on corresponding claims 2-6 of ('763). As per claim 4, ('763) uses the term 8-bit while in ('300) octets. These terms are synonymous. As per claims 3 and 6 the term cryptosynchronization value ('300) reads on the external value ('763). Synchronization between two cryptoprocessors must be made by a comparison of the two processor and hence occurs external to the two processors, hence it is an external value.

27. Claim 7 of ('763) differs from claim 7 of ('300), in that the former recites a permutation instead of bit rotation. However, the examiner asserts that a bit rotation is a special form of a bit rotation (i.e. a cyclic permutation on one bit).

28. Claims 9-15 of ('763) differ from claims 9-15 of claims of ('300) in that the former recites an inverse transformation and the latter a reverse transformation. The examiner asserts that these would be the same given the form of transformation being performed (e.g. involutions are self-inverting).

29. In claims 17 and 18, both ('763) and ('300) differ in that ('763) recites a first and second transformation whereas ('300) recites a transformation and inverse transformation. This differ was discussed in 25.

30. Claims1-6 are of application 09120763 is an obvious variation of claim 1 of patent US 6,233,337 and further in view of Reeds (EP 0532228 A2) and Laufer and is rejected as nonstatutory double patenting.

31. Claim 1 of ('763) recites a method for CMEA encryption or decryption cryptoprocessing to be employed in a wireless telephone system comprising:

- generating one or more offsets.
- inputting a message to a first transformation
- performing an iterative CMEA on it empolying an enhanced tbox (employing involution lookup) being subject to permutations of one or more offsets and
- performing a second transformation

32. Claim 1 of (US'337) discloses a CMEA encryption system to be empolyed in a wireless telephone system comprising:

- Generating a first and second offset (and claim 2 broaden this to a plurality)
- Inputting a message
- Applying a tbox function to a permutation being subject to permutation of the first and second offsets
- Performing a tbox function on the permuted results

33. Claim 1 of (US'337) differs from ('763) in that the transformation before the tbox is missing and (US'337) is silent on the use of involution lookup to enhance the tbox. Performing a tbox function on the permuted results would constitute a second transformation.

34. Reeds discloses a three stage (3 transformation) with the second stage involving an involution (an enhanced tbox, Figure 5c). One of ordinary skill in the art would have been motivated to combine a third stage (i.e. a first transformation ahead of the enhanced tbox) as this would provide greater security in that an arbitrary first

transformation involution would apply an independent action on the plaintext which would obfuscate the involution. Reeds is silent on the use of table lookup to implement involution. Laufer (Discrete Mathematics and Applied Modern Algebra) provides a method of evaluating involutions involving table lookup. With discrete functions table lookup is ultimately the only way to impliment involution or other discrete logic operations. Claim 1 of ('763) thus reads on (US'337)/Reeds/Laufer.

35. Claims 2 recites a first and second secret offset. Claim 1 of (US'337) discloses this.

36. Claim 3, combining the first and second secret value with and external value. Claim 3 of (US'337) discloses combining the first and second secret offsets with secret values generated from a pair of previously encrypted message octets (and therefore external).

37. Reeds discloses this (see above).

38. Claims 4-6 differ in that ('337) from those in ('763) in that 15/16 bit and 4 offsets as opposed to 8-bit and 2 offset. ('337) modified by Reeds and obvious changes meets limitation ('763).

Response to Arguments

39. Applicant's response in mute in view of new prior art.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to James Seal whose telephone number is 703 308 4562. The examiner can normally be reached on M-F, 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gail Hayes can be reached on 703 305 9711. The fax phone numbers for the organization where this application or proceeding is assigned are 703 305 0040 for regular communications and 703 305 0040 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703 308 3900.

JWS

jws
June 15, 2001

Gail Hayes

GAIL HAYES
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100